Docket No.: 60188-806 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Taichi NAGATA, et al.	:	Confirmation Number:
Serial No.:	:	Group Art Unit:
Filed: March 15, 2004	:	Examiner: Unknown

For: ACCESS CONTROL SYSTEM FOR NONVOLATILE MEMORY

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2003-075714, filed March 19, 2003

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:tlb
Facsimile: (202) 756-8087
Date: March 15, 2004

60188-806
March 15, 2004
NAGATA, et al.

日 本 国 特 許 庁
JAPAN PATENT OFFICE

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年 ３月１９日

出 願 番 号
Application Number: 特願２００３－０７５７１４

[ST. 10/C]: [ＪＰ２００３－０７５７１４]

出 願 人
Applicant(s): 松下電器産業株式会社

２００４年 ２月 ３日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００４－３００５５９１

【書類名】　特許願
【整理番号】　5037640176
【提出日】　平成15年 3月19日
【あて先】　特許庁長官　　殿
【国際特許分類】　G06F 12/06
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　　松下電器産業株式会社内
　【氏名】　永田　太一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　　松下電器産業株式会社内
　【氏名】　根本　祐輔
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100077931
　【弁理士】
　【氏名又は名称】　前田　　弘
【選任した代理人】
　【識別番号】　100094134
　【弁理士】
　【氏名又は名称】　小山　　廣毅
【選任した代理人】
　【識別番号】　100110939
　【弁理士】
　【氏名又は名称】　竹内　宏

【選任した代理人】

【識別番号】　100110940

【弁理士】

【氏名又は名称】　嶋田　高久

【選任した代理人】

【識別番号】　100113262

【弁理士】

【氏名又は名称】　竹内　祐二

【選任した代理人】

【識別番号】　100115059

【弁理士】

【氏名又は名称】　今江　克実

【選任した代理人】

【識別番号】　100115691

【弁理士】

【氏名又は名称】　藤田　篤史

【選任した代理人】

【識別番号】　100117581

【弁理士】

【氏名又は名称】　二宮　克也

【選任した代理人】

【識別番号】　100117710

【弁理士】

【氏名又は名称】　原田　智雄

【選任した代理人】

【識別番号】　100121500

【弁理士】

【氏名又は名称】　後藤　高志

【選任した代理人】

【識別番号】　100121728

【弁理士】

【氏名又は名称】　井関　勝守

【手数料の表示】

【予納台帳番号】　014409

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0217869

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　不揮発性メモリのアクセス制御システム

【特許請求の範囲】

【請求項１】　不揮発性メモリと、

システム初期化のためのプログラムを格納したブートＲＯＭと、

前記不揮発性メモリへのコマンドを発行するためのＣＰＵと、

前記ＣＰＵからコマンドを受け取って前記不揮発性メモリへのアクセスを制御するためのアクセス制御回路とを備え、

前記ＣＰＵは、システムの電源起動ごとに、前記ブートＲＯＭに格納したシステム初期化のためのプログラムを実行することにより前記不揮発性メモリ上に書き換え禁止領域を、当該書き換え禁止領域上に書き込み済みフラグをそれぞれ１回だけ設定するように動作し、

前記アクセス制御回路は、前記書き込み済みフラグの状態を確認するまでは前記不揮発性メモリの如何なる書き込みも認めず、前記書き込み済みフラグの状態を確認した後は、前記書き込み済みフラグが書き換え禁止を示さなければ前記書き換え禁止領域への書き込みを何度でも許可するが、前記書き込み済みフラグに書き換え禁止を設定した後は前記書き換え禁止領域への書き込みを一切認めないことを特徴とする不揮発性メモリのアクセス制御システム。

【請求項２】　請求項１記載のアクセス制御システムにおいて、

前記アクセス制御回路は、前記ＣＰＵから受け取ったコマンドを解析するためのコマンド解析部を有し、

前記コマンド解析部は、前記ＣＰＵから受け取ったコマンドが前記不揮発性メモリの書き込み又は消去を示し、その書き込み先又は消去先が前記不揮発性メモリの書き換え禁止領域であり、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記ＣＰＵから受け取ったコマンドを前記不揮発性メモリに伝達しないことを特徴とするアクセス制御システム。

【請求項３】　請求項２記載のアクセス制御システムにおいて、

前記コマンド解析部は、前記不揮発性メモリの書き込み又は消去に特別なコマンド列を必要とする場合には、前記ＣＰＵから受け取った全てのコマンドを解析

し、当該コマンド列が前記不揮発性メモリの書き込み又は消去を示し、その書き込み先又は消去先が前記不揮発性メモリの書き換え禁止領域であり、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記ＣＰＵから受け取ったコマンド列を前記不揮発性メモリに一切伝達しないことを特徴とするアクセス制御システム。

【請求項４】　請求項２記載のアクセス制御システムにおいて、

前記コマンド解析部は、前記不揮発性メモリの全消去に特別なコマンド列を必要とする場合には、前記ＣＰＵから受け取った全てのコマンドを解析し、当該コマンド列が前記不揮発性メモリの全消去を示し、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記ＣＰＵから受け取ったコマンド列を前記不揮発性メモリに一切伝達しないことを特徴とするアクセス制御システム。

【請求項５】　請求項１記載のアクセス制御システムにおいて、

前記不揮発性メモリ上に有用なデータを置かない未使用領域が設けられ、

前記アクセス制御回路は、前記ＣＰＵから受け取ったコマンドを解析するためのコマンド解析部を有し、

前記コマンド解析部は、前記ＣＰＵから受け取ったコマンドが前記不揮発性メモリの書き込み又は消去を示し、その書き込み先又は消去先が前記不揮発性メモリの書き換え禁止領域であり、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記不揮発性メモリの未使用領域に対して書き込み又は消去を行うように制御することを特徴とするアクセス制御システム。

【請求項６】　請求項５記載のアクセス制御システムにおいて、

前記コマンド解析部は、前記不揮発性メモリの書き込み又は消去に特別なコマンド列を必要とする場合には、前記ＣＰＵから受け取った全てのコマンドを解析し、当該コマンド列が前記不揮発性メモリの書き込み又は消去を示し、その書き込み先又は消去先が前記不揮発性メモリの書き換え禁止領域であり、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記不揮発性メモリの未使用領域に対して書き込み又は消去を行うように制御することを特徴とするアクセス制御システム。

【請求項７】　請求項５記載のアクセス制御システムにおいて、

前記コマンド解析部は、前記不揮発性メモリの全消去に特別なコマンド列を必要とする場合には、前記ＣＰＵから受け取った全てのコマンドを解析し、当該コマンド列が前記不揮発性メモリの全消去を示し、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記不揮発性メモリの未使用領域に対して全消去を行うように制御することを特徴とするアクセス制御システム。

【請求項８】　請求項１記載のアクセス制御システムにおいて、

前記アクセス制御回路は、前記不揮発性メモリ上の書き換え禁止領域に対する書き込み又は消去を検知し、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記不揮発性メモリ上の書き換え禁止領域を除く領域中のデータを消去するように制御することを特徴とするアクセス制御システム。

【請求項９】　請求項１記載のアクセス制御システムにおいて、

前記アクセス制御回路は、前記不揮発性メモリ上の書き換え禁止領域に対する書き込み又は消去を検知し、かつ前記書き込み済みフラグが書き換え禁止を示す場合には、前記不揮発性メモリ上の全データを前記書き込み済みフラグと同じ値に書き換えるように制御することを特徴とするアクセス制御システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、不揮発性メモリのアクセス制御システムに関するものである。

【０００２】

【従来の技術】

ある従来技術によれば、課金情報、残金情報などを記憶するための不揮発性メモリに特定アドレスの書き込み回数制限回路を設けることで、ＩＣカードの不正使用を防止する（特許文献１参照）。

【０００３】

他の従来技術によれば、不揮発性メモリ上にデータとプログラムとを混在させ得るように、特定アドレス領域のみデータの書き換えを可能とし、プログラム格納のための他のアドレス領域ではハードウェアにて書き換えを禁止する（特許文献２参照）。

【０００４】

【特許文献１】

特開平８－３２９２０８号公報

【特許文献２】

特開平１１－１１０２８７号公報

【０００５】

【発明が解決しようとする課題】

例えば携帯電話において音楽、映画などの有料コンテンツの配信を受ける場合には、ユーザＩＤ及びパスワードといった個人認証情報が必要である。また、暗号化されたコンテンツを復号するためには鍵情報が必要である。これらの情報を不揮発性メモリに格納して利用する場合には、その改竄を防止するセキュリティ対策が重要である。

【０００６】

ところが、上記特定アドレスの書き込み回数制限回路を不揮発性メモリに設ける従来技術では、システム作成者が改竄防止を必要とする情報の書き込みに失敗した場合に、再書き込みが不能になるおそれがある。

【０００７】

本発明の目的は、システム作成者が改竄防止を必要とする情報の書き込みを自由にでき、かつ当該情報の改竄を確実に防止できる不揮発性メモリのアクセス制御システムを提供することにある。

【０００８】

【課題を解決するための手段】

上記目的を達成するため、本発明は、ブートＲＯＭに格納したシステム初期化のためのプログラムに従ってＣＰＵが不揮発性メモリ上に書き換え禁止領域を設定し、かつ当該書き換え禁止領域上に設定した書き込み済みフラグに従ってアクセス制御回路が書き換え許可／禁止の制御を行うこととしたものである。

【０００９】

具体的に説明すると、本発明は、不揮発性メモリと、システム初期化のためのプログラムを格納したブートＲＯＭと、不揮発性メモリへのコマンドを発行する

ためのＣＰＵと、当該ＣＰＵからコマンドを受け取って不揮発性メモリへのアクセスを制御するためのアクセス制御回路とを備えた構成を採用し、ＣＰＵは、システムの電源起動ごとに、ブートＲＯＭに格納したシステム初期化のためのプログラムを実行することにより不揮発性メモリ上に書き換え禁止領域を、当該書き換え禁止領域上に書き込み済みフラグをそれぞれ１回だけ設定するように動作し、アクセス制御回路は、書き込み済みフラグの状態を確認するまでは不揮発性メモリの如何なる書き込みも認めず、書き込み済みフラグの状態を確認した後は、当該書き込み済みフラグが書き換え禁止を示さなければ書き換え禁止領域への書き込みを何度でも許可するが、当該書き込み済みフラグに書き換え禁止を設定した後は書き換え禁止領域への書き込みを一切認めないこととしたものである。

【００１０】

【発明の実施の形態】

以下、添付図面を参照しながら本発明の実施形態を詳細に説明する。

【００１１】

図１は、本発明に係る不揮発性メモリのアクセス制御システムの全体構成例を示している。図１の不揮発性メモリのアクセス制御システム１において、２はＣＰＵ、３はＳＲＡＭ、４はブートＲＯＭ、５はアクセス制御回路、６は不揮発性メモリ、７はシステムバスである。ＣＰＵ２、ＳＲＡＭ３及びブートＲＯＭ４は、システムバス７に接続されている。アクセス制御回路５は、不揮発性メモリ６とシステムバス７との間に介在する。ＳＲＡＭ３は、プログラム又はデータを格納するためのメモリである。ブートＲＯＭ４は、システム初期化のためのプログラムを格納したメモリである。不揮発性メモリ６は、例えばフラッシュメモリである。ＣＰＵ２は、ＳＲＡＭ３に格納したプログラム又はブートＲＯＭ４に格納したプログラムを実行することにより、不揮発性メモリ２へのアクセスのためのコマンドを発行する。アクセス制御回路５は、ＣＰＵ２からコマンドを受け取って不揮発性メモリ６へのアクセスを制御するための回路である。

【００１２】

図２は、図１中の不揮発性メモリ６の内部構成を示している。不揮発性メモリ６は、例えばアドレス００００ｈから７ＦＦＦｈまでの書き換え可能領域と、ア

ドレス８０００ｈからＦＦＦＦｈまでの書き換え禁止領域とに分割される（ｈは１６進数表記：以下同じ）。更に、書き換え禁止領域上の例えばアドレスＦＦＦ０ｈで指定される１バイト中に１ビットの書き込み済みフラグＦが設定される。以下の説明では、不揮発性メモリ６の初期状態では全ビットの値が「１」であるものとする。したがって、書き込み済みフラグＦの初期値も「１」である。ここでは、「Ｆ＝１」が書き換え許可を、「Ｆ＝０」が書き換え禁止をそれぞれ示すものとする。

【００１３】

図３は、図１中のアクセス制御回路５の内部構成を示している。図３のアクセス制御回路５は、レジスタファイル１０と、コマンド解析部２０と、ライト／リード信号発行部３０とを備えている。レジスタファイル１０は、書き換え禁止領域アドレスレジスタ１１と、書き換え禁止領域アドレスマスクレジスタ１２と、書き換え禁止セクタアドレスレジスタ１３と、書き込み済みフラグアドレスレジスタ１４と、書き込み済みフラグビットレジスタ１５と、書き込み済みフラグチェックコマンドレジスタ１６と、レジスタステートマシン１７とを有するものである。コマンド解析部２０は、ＣＰＵ２からシステムバス７を介して受け取ったコマンドを、レジスタファイル１０を参照しながら解析する。ライト／リード信号発行部３０は、コマンド解析部２０での解析結果に従って不揮発性メモリ６の書き込み（ライト）／読み出し（リード）／消去（イレーズ）のための信号を発行する。特に不揮発性メモリ６上の書き込み済みフラグＦを含む１バイトにアクセスする場合には、ライト／リード信号発行部３０は、書き込み済みフラグアドレスレジスタ１４と、書き込み済みフラグチェックコマンドレジスタ１６とを参照する。

【００１４】

図１中のＣＰＵ２は、システムの電源起動ごとに、ブートＲＯＭ４に格納したシステム初期化のためのプログラムを実行することにより不揮発性メモリ６上に書き換え禁止領域を、当該書き換え禁止領域上に書き込み済みフラグＦをそれぞれ１回だけ設定するように動作する。図２の例に従えば、書き換え禁止領域アドレスレジスタ１１に８０００ｈが、書き換え禁止領域アドレスマスクレジスタ１

２に７ＦＦＦｈがそれぞれ設定される。また、書き込み済みフラグアドレスレジスタ１４にＦＦＦ０ｈが、書き込み済みフラグビットレジスタ１５に３ｈがそれぞれ設定される。

【００１５】

図３のアクセス制御回路５は、ＣＰＵ２から書き込み済みフラグチェックコマンドが与えられて書き込み済みフラグＦの状態を確認するまでは不揮発性メモリ６の如何なる書き込みも認めず、書き込み済みフラグＦの状態を確認した後は、当該書き込み済みフラグＦが書き換え許可（Ｆ＝１）を示す限りは書き換え禁止領域への書き込みを何度でも許可するが、当該書き込み済みフラグＦに書き換え禁止（Ｆ＝０）を設定した後は書き換え禁止領域への書き込みを一切認めないように動作する。したがって、システム作成者が改竄防止を必要とする情報の書き込みを自由にでき、かつ当該情報の改竄を確実に防止できる。

【００１６】

図３中のコマンド解析部２０は、ＣＰＵ２から受け取ったコマンドが不揮発性メモリ６の書き込み又は消去を示し、その書き込み先又は消去先が不揮発性メモリ６の書き換え禁止領域であり、かつ書き込み済みフラグＦが書き換え禁止（Ｆ＝０）を示す場合には、ＣＰＵ２から受け取ったコマンドをライト／リード信号発行部３０に伝達しないように動作する。

【００１７】

図４は、図３中のレジスタステートマシン１７の動作を示している。レジスタステートマシン１７は初期状態として、状態１にある。状態１においてＣＰＵ２により書き換え禁止領域アドレスレジスタ１１が設定されると、状態２に遷移する。設定されなければ状態１を保つ。状態２において書き換え禁止領域アドレスマスクレジスタ１２が設定されると、状態３に遷移する。設定されなければ状態２を保つ。状態３において書き換え禁止セクタアドレスレジスタ１３が設定されると、状態４に遷移する。設定されなければ状態３を保つ。状態４において書き込み済みフラグアドレスレジスタ１４が設定されると、状態５に遷移する。設定されなければ状態４を保つ。状態５において書き込み済みフラグビットレジスタ１５が設定されると、状態６に遷移する。設定されなければ状態５を保つ。

【００１８】

状態６になって始めて、書き込み済みフラグチェックコマンドレジスタ１６はシステムバス７からの書き込みを受け付ける。書き込み済みフラグチェックコマンドレジスタ１６に書き込み済みフラグＦの状態確認実行のためのコマンドが設定されると、書き込み済みフラグチェックコマンドレジスタ１６はそれをライト／リード信号発行部３０に伝え、ライト／リード信号発行部３０は書き込み済みフラグアドレスレジスタ１４に設定されたアドレスのデータを不揮発性メモリ６よりリードする。コマンド解析部２０は、リードしたデータのうち書き込み済みフラグビットレジスタ１５で示されるビットの値を書き込み済みフラグＦとして保持する。

【００１９】

レジスタステートマシン１７を状態１から状態６へ遷移させ、かつ書き込み済みフラグチェックコマンドを発行することによりコマンド解析部２０に書き込み済みフラグＦを保持させる上記処理は、ブートＲＯＭ４に格納したシステム初期化のためのプログラムをＣＰＵ２が実行することにより達成される。これらの処理が全て完了するまでは、システムバス７から不揮発性メモリ６への如何なる書き込み、消去をもコマンド解析部２０により禁止する。

【００２０】

書き込み済みフラグＦをチェックした後のライト／消去の可否判断はコマンド解析部２０で行う。具体的には、書き込み済みフラグＦが書き込み許可（Ｆ＝１）を示すなら、コマンド解析部２０は、書き換え禁止領域アドレスレジスタ１１と書き換え禁止領域アドレスマスクレジスタ１２とによって示される不揮発性メモリ６の書き換え禁止領域への書き込み、書き換え禁止セクタアドレスレジスタ１３によって設定されるセクタの消去、不揮発性メモリ６上の全領域のイレーズのいずれをも許可する。したがって、システム作成者は、自分で不揮発性メモリ６上の書き込み済みフラグＦを「０」に書き換えるまでは、改竄防止を必要とする情報の書き換え禁止領域への書き込みを自由にできる。しかし、システム作成者が不揮発性メモリ６上の書き込み済みフラグＦを「０」に書き換えた後は、コマンド解析部２０は、書き換え禁止領域への如何なる書き込み、消去も許可しな

い。なお、不揮発性メモリ６上の書き込み済みフラグＦのコピーをコマンド解析部２０が常に保持することとすれば、書き込み済みフラグチェックコマンドの発行回数を削減できる。

【００２１】

図５は、図１中の不揮発性メモリ６のコマンドの例を示している。この不揮発性メモリ６は、ライト及びイレーズにそれぞれ特別なコマンド列を必要とするフラッシュメモリである。図５中のＡＤＲＳはＣＰＵ２が発行するアドレスを、ＤＡＴＡはＣＰＵ２が発行するデータをそれぞれ表す。

【００２２】

図５の上段に示すように、ライトコマンドにおいては、１サイクル目にアドレス５５５ｈ／データＡＡｈが、２サイクル目にアドレス２ＡＡｈ／データ５５ｈが、３サイクル目にアドレス５５５ｈ／データＡ０ｈがそれぞれ入力された場合に、４サイクル目に入力されたアドレスＷＡに４サイクル目に入力されたデータＷＤをライトするように決められている。

【００２３】

図５の中段に示すように、セクタイレーズコマンドにおいては、１サイクル目に５５５ｈ／データＡＡｈが、２サイクル目にアドレス２ＡＡｈ／データ５５ｈが、３サイクル目にアドレス５５５ｈ／データ８０ｈが、４サイクル目にアドレス５５５ｈ／データＡＡｈが、５サイクル目にアドレス２ＡＡｈ／データ５５ｈが、６サイクル目にデータ３０ｈがそれぞれ入力された場合に、６サイクル目にデータ３０ｈとともに入力されるアドレスＳＡで指定されたセクタのイレーズを行うように決められている。

【００２４】

図５の下段に示すように、チップイレーズコマンドにおいては、５サイクル目まではセクタイレーズコマンドと同様であり、６サイクル目にアドレス５５５ｈ／データ１０ｈが入力された場合に、不揮発性メモリ６上の全領域のイレーズを行うように決められている。

【００２５】

図６は、図３中のコマンド解析部２０の動作を示している。コマンド解析部２

０は初期状態として、状態１にある。状態１においてシステムバス７よりアドレス５５５ｈ／データＡＡｈが入力されると、状態２に遷移する。それ以外の入力がなされた場合には状態１を保持する。状態２においてアドレス２ＡＡｈ／データ５５ｈが入力されると、状態３に遷移する。それ以外の入力がなされた場合には状態１に遷移する。

【００２６】

状態３においてアドレス５５５ｈ／データＡ０ｈが入力されると、状態４．１に遷移する。状態４．１は、システムバス７より正常なライトコマンドが入力されたことを表す状態である。状態４．１においては、その次に入力されたアドレスＷＡが書き換え禁止領域アドレスレジスタ１１及び書き換え禁止領域アドレスマスクレジスタ１２により設定された不揮発性メモリ６の書き換え禁止領域に相当するかどうかをコマンド解析部２０が判断する。禁止領域に相当する場合には、そのアドレスへのライトは行わない。禁止領域に相当しない場合にはそのアドレスへのデータＷＤのライトを行う。

【００２７】

状態３においてアドレス５５５ｈ／データ８０ｈが入力されると、状態４．２に遷移する。それ以外の入力がなされた場合には状態１に遷移する。状態４．２においてアドレス５５５ｈ／データＡＡｈが入力されると、状態５に遷移する。それ以外の入力がなされた場合には状態１に遷移する。状態５においてアドレス２ＡＡｈ／データ５５ｈが入力されると、状態６に遷移する。それ以外の入力がなされた場合には状態１に遷移する。

【００２８】

状態６においてアドレス５５５ｈ／データ１０ｈが入力されると、それはチップイレーズを表す。不揮発性メモリ６上の書き込み済みフラグＦが書き換え許可（Ｆ＝１）を示す限り、コマンド解析部２０は不揮発性メモリ６へのチップイレーズコマンドの発行を行う。しかしながら、不揮発性メモリ６上の書き込み済みフラグＦを「０」に書き換えた後には当該不揮発性メモリ６のチップイレーズは禁止するので、コマンド解析部２０は不揮発性メモリ６へのイレーズコマンドの発行を行わない。

【００２９】

状態６においてデータ３０ｈが入力されると、それはセクタイレーズを表す。よって、そのときに入力されたセクタアドレスＳＡが書き換え禁止セクタアドレスレジスタ１３に設定されたセクタアドレスと異なる場合には、これに対応するセクタイレーズコマンドをコマンド解析部２０が不揮発性メモリ６に発行する。書き換え禁止セクタアドレスレジスタ１３に設定されたセクタアドレスと同一の場合には、そのセクタのイレーズは禁止するので、コマンド解析部２０は不揮発性メモリ６へのコマンド発行を行わない。状態６においてそれ以外の入力がなされた場合には、状態１に遷移する。

【００３０】

コマンド解析部２０では全コマンドが正常に入力され、かつＣＰＵ２がライトしようとするアドレス、又はＣＰＵ２がイレーズしようとするセクタアドレスが禁止領域でないと判明してから、それまで溜め込んでおいた全てのコマンドを最初から順次ライト／リード信号発行部３０に与える。したがって、ライト／リード信号発行部３０へはアクセスの許可されたコマンドしか入力されないので、ライト／リード信号発行部３０は、コマンド解析部２０より入力される全てのアドレス／データをそのまま不揮発性メモリ６へ出力することができる。

【００３１】

以上のとおり、システムバス７より入力されたアドレス／データをアクセス制御回路５にて解析し、アクセスを許可した場合にのみ不揮発性メモリ６へのライト／イレーズを行う。

【００３２】

詳細に言うと、コマンド解析部２０は、ＣＰＵ２から受け取った全てのコマンドを解析し、受け取ったコマンド列が不揮発性メモリ６のライト又はセクタイレーズを示し、そのライト先又はイレーズ先が書き換え禁止領域であり、かつ書き込み済みフラグＦが書き換え禁止を示す場合には、ＣＰＵ２から受け取ったコマンド列を不揮発性メモリ６に一切伝達しない。また、コマンド解析部２０は、ＣＰＵ２から受け取ったコマンド列が不揮発性メモリ６のチップイレーズを示し、かつ書き込み済みフラグＦが書き換え禁止を示す場合には、ＣＰＵ２から受け取

ったコマンド列を不揮発性メモリ６に一切伝達しないのである。

【００３３】

なお、図１中のブートＲＯＭ４のプログラムを差し替えることで図２中のレジスタファイル１０の設定変更を実現すれば、不揮発性メモリ６上の書き換え禁止領域の設定をシステム毎に任意に変更できる。例えば、書き換え禁止領域アドレスレジスタ１１に４０００ｈを、書き換え禁止領域アドレスマスクレジスタ１２に３ＦＦＦｈをそれぞれ設定すれば、アドレス４０００ｈから７ＦＦＦｈまでの領域を書き換え禁止領域に設定することができる。

【００３４】

図７は、図１中の不揮発性メモリ６の他の内部構成を示している。ここでは、不揮発性メモリ６上に有用なデータを置かない未使用領域としてダミーセクタが設けられ、例えばアドレス００１０ｈがダミーバイトと定められる。

【００３５】

この場合、コマンド解析部２０は、ＣＰＵ２から受け取ったコマンド列が不揮発性メモリ６のライトを示し、そのライト先が書き換え禁止領域であり、かつ書き込み済みフラグＦが書き換え禁止を示す場合には、ダミーバイトに対して書き込みを行うように制御する。また、ＣＰＵ２から受け取ったコマンド列が不揮発性メモリ６のセクタイレーズを示し、そのイレーズ先が書き換え禁止領域であり、かつ書き込み済みフラグＦが書き換え禁止を示す場合には、ダミーセクタに対して書き込みを行うようにコマンド解析部２０が制御する。また、ＣＰＵ２から受け取ったコマンド列が不揮発性メモリ６のチップイレーズを示し、かつ書き込み済みフラグＦが書き換え禁止を示す場合にも、ダミーセクタに対して書き込みを行うようにコマンド解析部２０が制御する。

【００３６】

このようにコマンド解析部２０は、システムバス７より図５に示すアドレス／データを入力された都度、これをライト／リード信号発行部３０に出力しながら、書き換え可能領域のライト／イレーズの場合にはライト先／イレーズ先を変更せず、書き換え禁止領域のライト／イレーズの場合にはライト先／イレーズ先を変更することでライト／イレーズのシーケンスを完了する。つまり、書き換え可

能領域中の一部を犠牲にするだけで、コマンド解析部２０がコマンド列を一時的に溜め込んでおく図２の場合に比べて、不揮発性メモリ６のアクセス速度が向上するのである。

【００３７】

最後に、書き換え禁止領域中の情報を改竄しようとした者にペナルティを与えることができる構成を図８及び図９に示す。

【００３８】

図８は、図３中のコマンド解析部２０の内部構成図である。図８において、２１はコマンド出力部、２２はライト／消去コマンド検出部、２３はイレーズコマンド発行部である。コマンド出力部２１は、通常はＣＰＵ２からシステムバス７を介して受け取ったコマンドをそのままライト／リード信号発行部３０へ供給する。ライト／消去コマンド検出部２２は、書き換え禁止領域に対するライト／イレーズコマンドを検知し、かつ書き込み済みフラグＦが書き換え禁止（Ｆ＝０）を示す場合には、その旨をイレーズコマンド発行部２３に伝える。これに応答して、イレーズコマンド発行部２３は、図３中の書き換え禁止セクタアドレスレジスタ１３に設定されたセクタアドレス以外の全てのセクタに対するイレーズコマンド発行命令をコマンド出力部２１に与える。コマンド出力部２１は、この命令に従って各セクタイレーズコマンドを発行する。これにより、改竄を防止しつつ、改竄を試みた者にペナルティを与えるように書き換え可能領域中の有用な情報が消去される。

【００３９】

図９は、図３中のコマンド解析部２０の他の内部構成図である。図９では、図８中のイレーズコマンド発行部２３が書き込み済みフラグオーバーライト部２４に置き換えられている。この書き込み済みフラグオーバーライト部２４は、書き換え禁止領域に対するライト／イレーズコマンドを検知し、かつ書き込み済みフラグＦが書き換え禁止（Ｆ＝０）を示す旨をライト／消去コマンド検出部２２から伝えられた場合には、図３中の書き込み済みフラグチェックコマンドレジスタ１６に基づく状態確認実行により取得した書き込み済みフラグＦと同じ値（＝０）をライトデータとするように、全領域ライト命令をコマンド出力部２１に与え

る。コマンド出力部２１は、この命令に従って全領域ライトコマンドを発行する。これにより、改竄を試みた者にペナルティを与えるように、不揮発性メモリ６上の全データが書き込み済みフラグＦと同じ値（＝０）に書き換えられる。しかも、書き込み済みフラグＦそのものは依然として書き換え禁止（Ｆ＝０）を示すので、以後の書き込みも受け付けられない。

【００４０】

なお、不揮発性メモリ６の初期状態で全ビットの値が「０」であるなら、「Ｆ＝０」が書き換え許可を、「Ｆ＝１」が書き換え禁止をそれぞれ示すものとすればよい。

【００４１】

また、本発明はＥＥＰＲＯＭなどの他の種類の不揮発性メモリにも適用可能である。

【００４２】

【発明の効果】

以上説明してきたとおり、本発明によれば、ブートＲＯＭに格納したシステム初期化のためのプログラムに従ってＣＰＵが不揮発性メモリ上に書き換え禁止領域を設定し、かつ当該書き換え禁止領域上に設定した書き込み済みフラグに従ってアクセス制御回路が書き換え許可／禁止の制御を行うこととしたので、システム作成者が改竄防止を必要とする情報の書き込みを自由にでき、かつ当該情報の改竄を確実に防止できる不揮発性メモリのアクセス制御システムを提供できる。

【図面の簡単な説明】

【図１】

本発明に係る不揮発性メモリのアクセス制御システムの全体構成例を示すブロック図である。

【図２】

図１中の不揮発性メモリの内部構成図である。

【図３】

図１中のアクセス制御回路の内部構成図である。

【図４】

図３中のレジスタステートマシンの動作を示す状態遷移図である。

【図５】

図１中の不揮発性メモリのコマンド例を示す図である。

【図６】

図３中のコマンド解析部の動作を示す状態遷移図である。

【図７】

図１中の不揮発性メモリの他の内部構成図である。

【図８】

図３中のコマンド解析部の内部構成図である。

【図９】

図３中のコマンド解析部の他の内部構成図である。

【符号の説明】

１　不揮発性メモリのアクセス制御システム

２　ＣＰＵ

３　ＳＲＡＭ

４　ブートＲＯＭ

５　アクセス制御回路

６　不揮発性メモリ

７　システムバス

１０　レジスタファイル

１１　書き換え禁止領域アドレスレジスタ

１２　書き換え禁止領域アドレスマスクレジスタ

１３　書き換え禁止セクタアドレスレジスタ

１４　書き込み済みフラグアドレスレジスタ

１５　書き込み済みフラグビットレジスタ

１６　書き込み済みフラグチェックコマンドレジスタ

１７　レジスタステートマシン

２０　コマンド解析部

２１　コマンド出力部

２２　ライト／消去コマンド検出部

２３　イレーズコマンド発行部

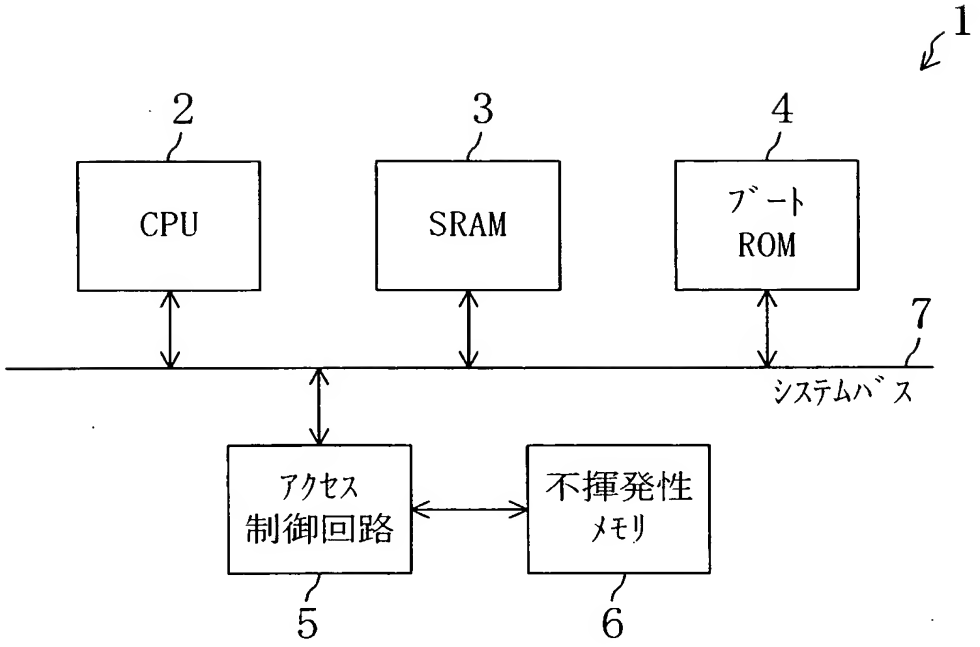
２４　書き込み済みフラグオーバーライト部

３０　ライト／リード信号発行部

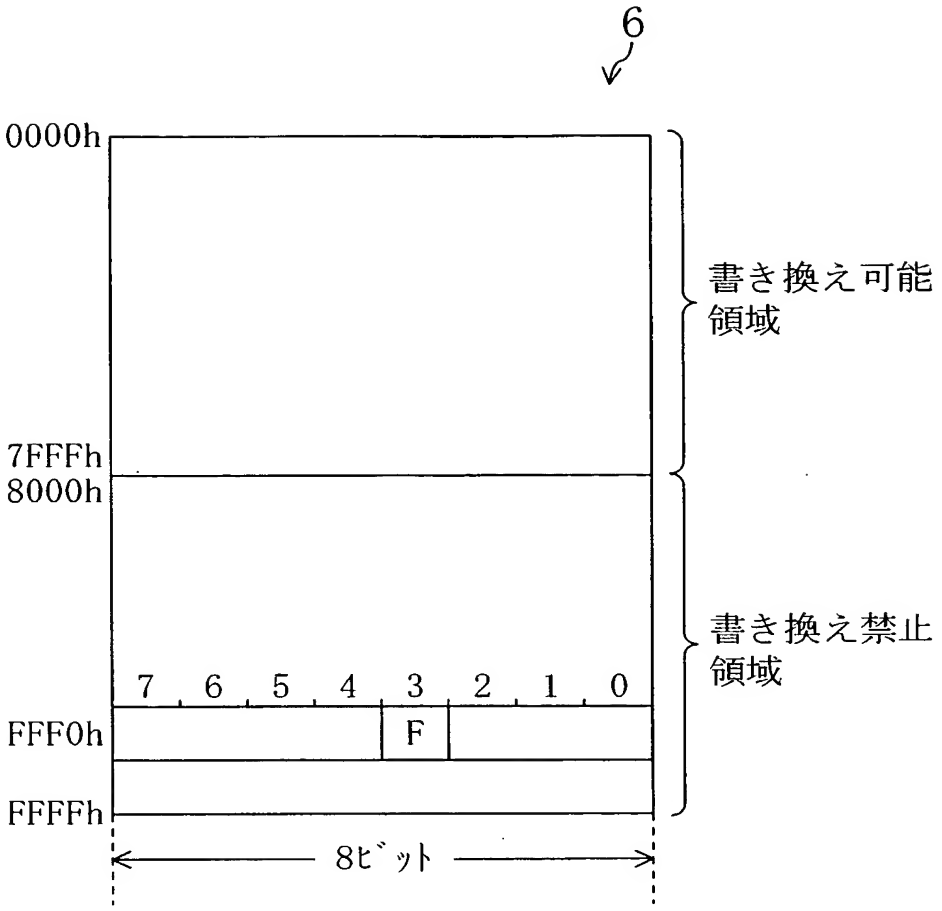
Ｆ　書き込み済みフラグ

【書類名】　図面

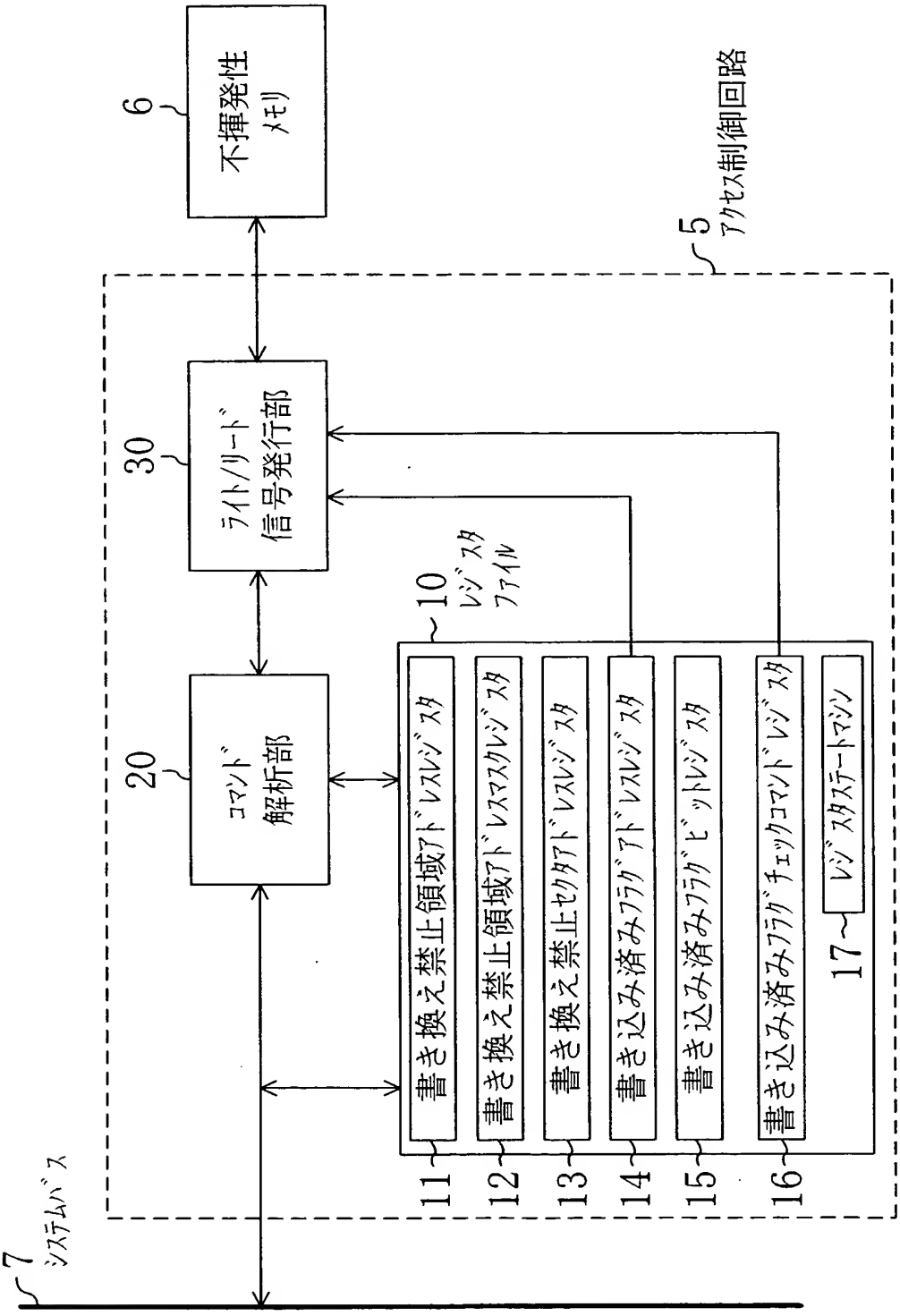
【図１】



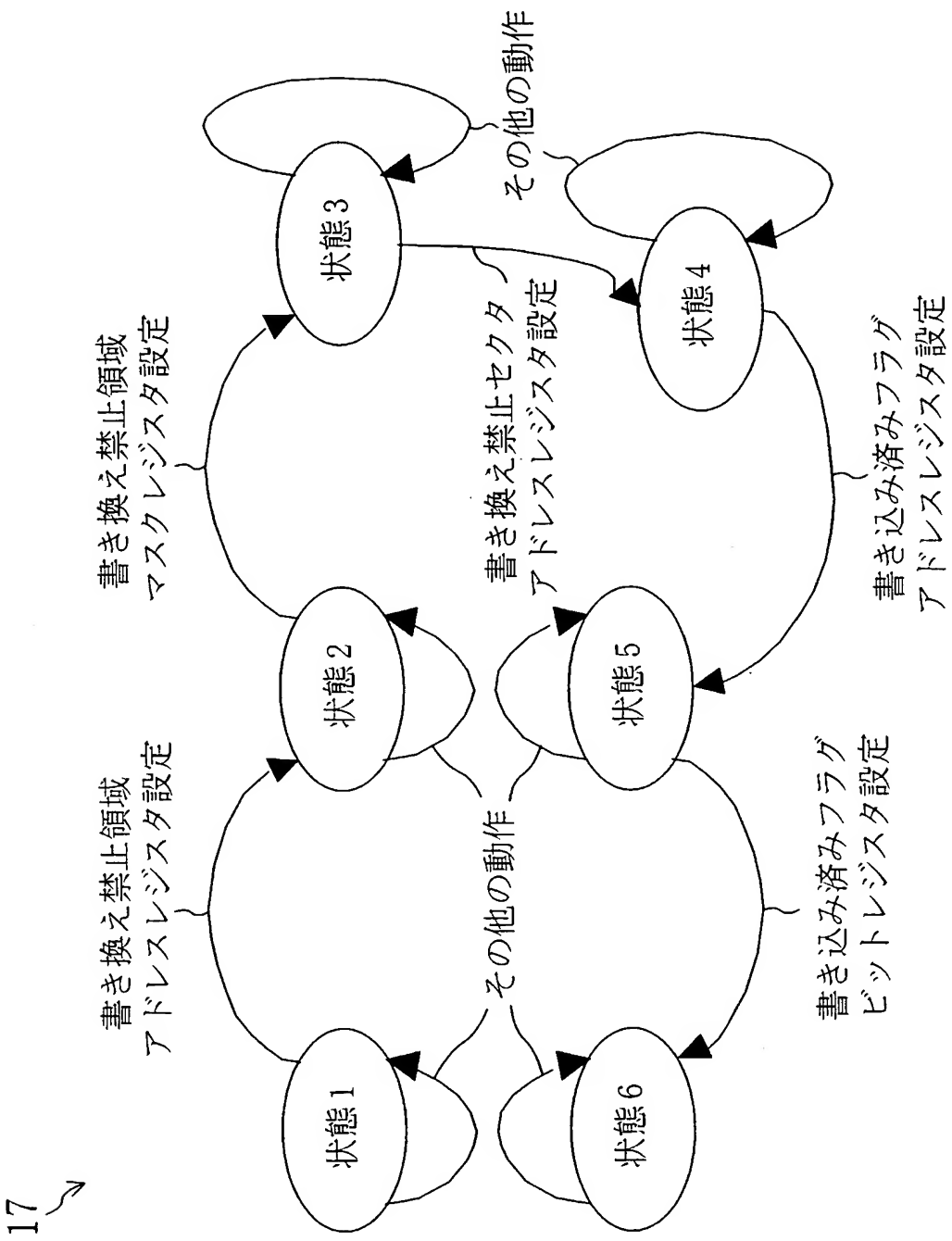
【図２】


6
0000h
7FFFh
8000h
FFF0h
FFFFh
7 6 5 4 3 2 1 0
F
8ビット
書き換え可能
領域
書き換え禁止
領域

【図３】


6
不揮発性
ﾒﾓﾘ
5
ｱｸｾｽ制御回路
30
ﾗｲﾄ/ﾘｰﾄﾞ
信号発行部
10
ﾚｼﾞｽﾀ
ﾌｧｲﾙ
20
ｺﾏﾝﾄﾞ
解析部
書き換え禁止領域ｱﾄﾞﾚｽﾚｼﾞｽﾀ
書き換え禁止領域ｱﾄﾞﾚｽﾏｽｸﾚｼﾞｽﾀ
書き換え禁止ｾｸﾀｱﾄﾞﾚｽﾚｼﾞｽﾀ
書き込み済みﾌﾗｸﾞｱﾄﾞﾚｽﾚｼﾞｽﾀ
書き込み済みﾌﾗｸﾞﾋﾞｯﾄﾚｼﾞｽﾀ
書き込み済みﾌﾗｸﾞﾁｪｯｸｺﾏﾝﾄﾞﾚｼﾞｽﾀ
ﾚｼﾞｽﾀｽﾃｰﾄﾏｼﾝ
11
12
13
14
15
16
17
7
ｼｽﾃﾑﾊﾞｽ

【図４】

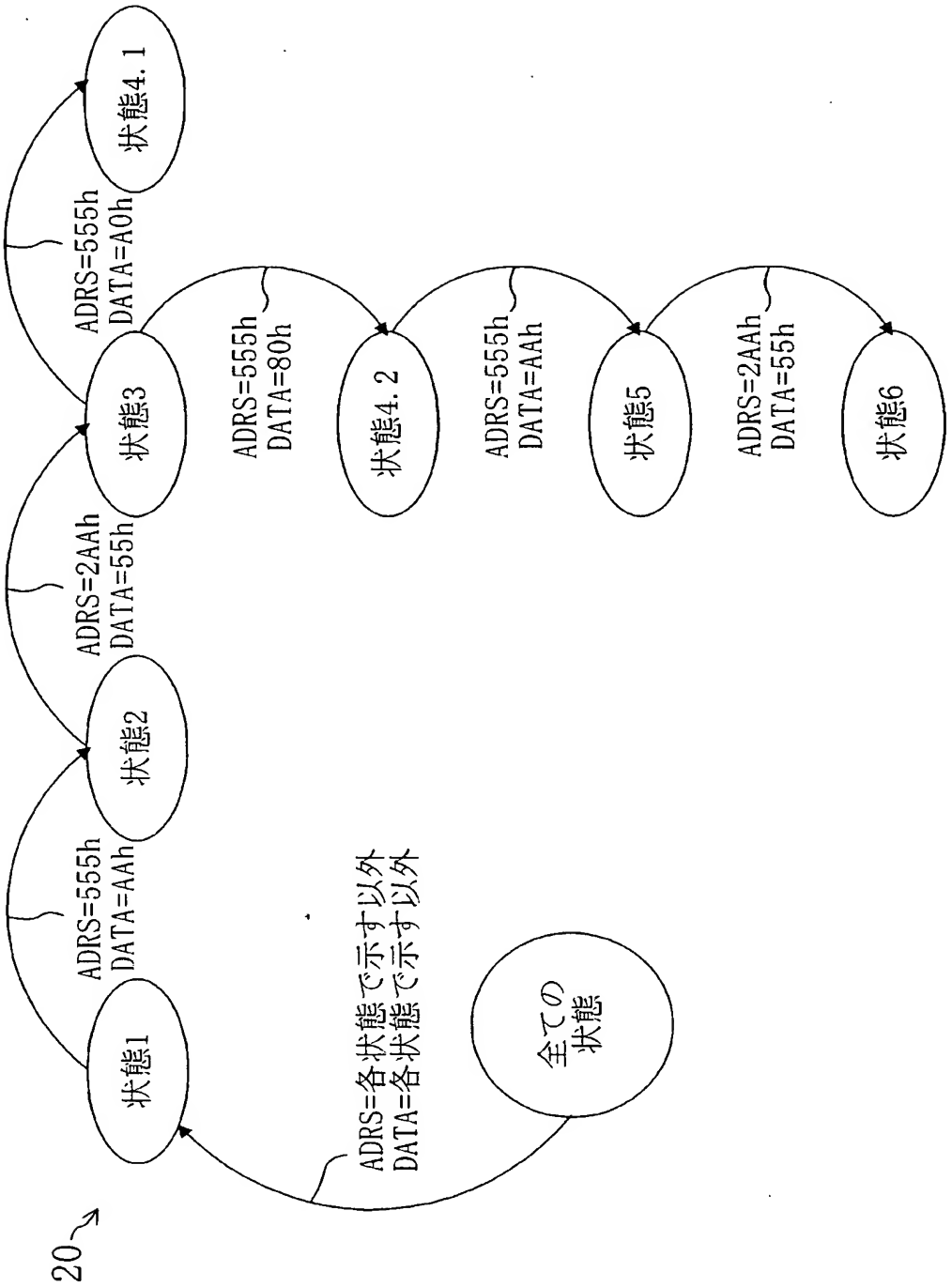

17
状態1
状態2
状態3
状態4
状態5
状態6
書き換え禁止領域
アドレスレジスタ設定
その他の動作
書き換え禁止領域
マスクレジスタ設定
書き換え禁止セクタ
アドレスレジスタ設定
その他の動作
書き込み済みフラグ
ビットレジスタ設定
書き込み済みフラグ
アドレスレジスタ設定

【図５】

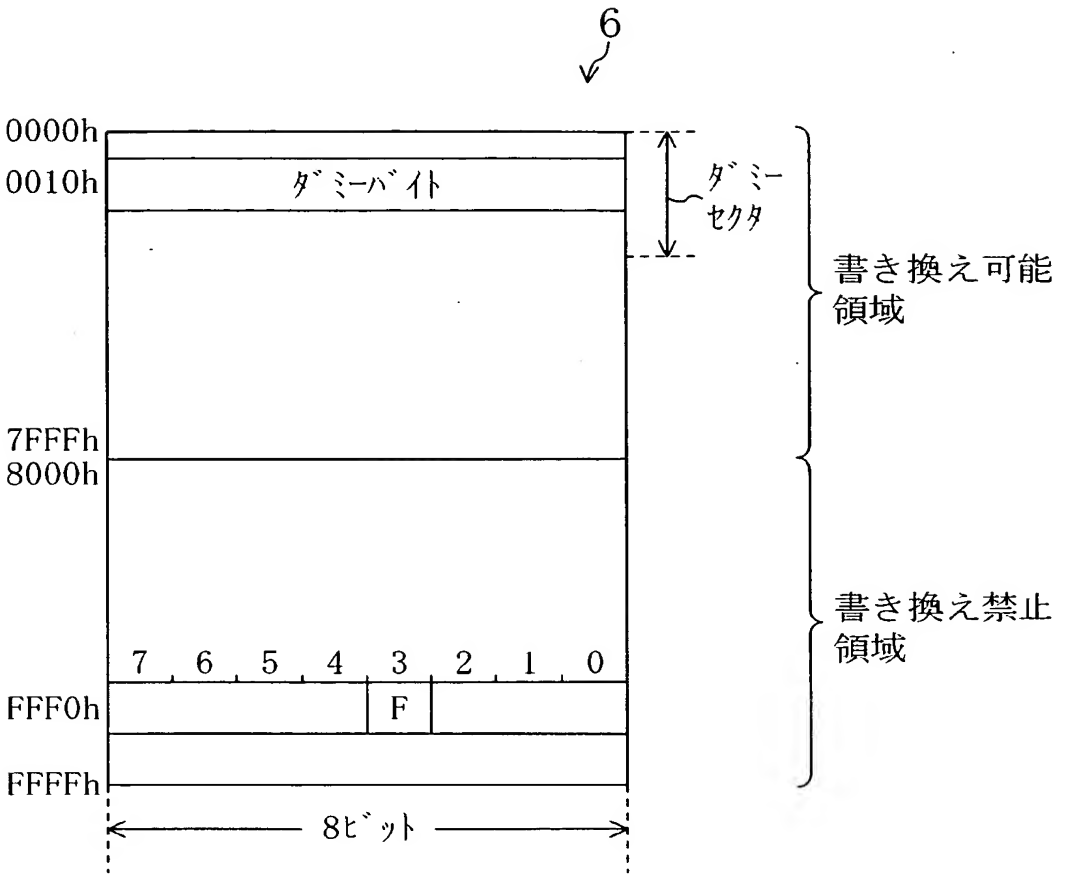
サイクル		1	2	3	4	5	6
ライト	ADRS	555h	2AAh	555h	WA	－	－
	DATA	AAh	55h	A0h	WD	－	－
セクタイレーズ	ADRS	555h	2AAh	555h	555h	2AAh	SA
	DATA	AAh	55h	80h	AAh	55h	30h
チップイレーズ	ADRS	555h	2AAh	555h	555h	2AAh	555h
	DATA	AAh	55h	80h	AAh	55h	10h

WA:ライトアドレス
WD:ライトデータ
SA:セクタアドレス

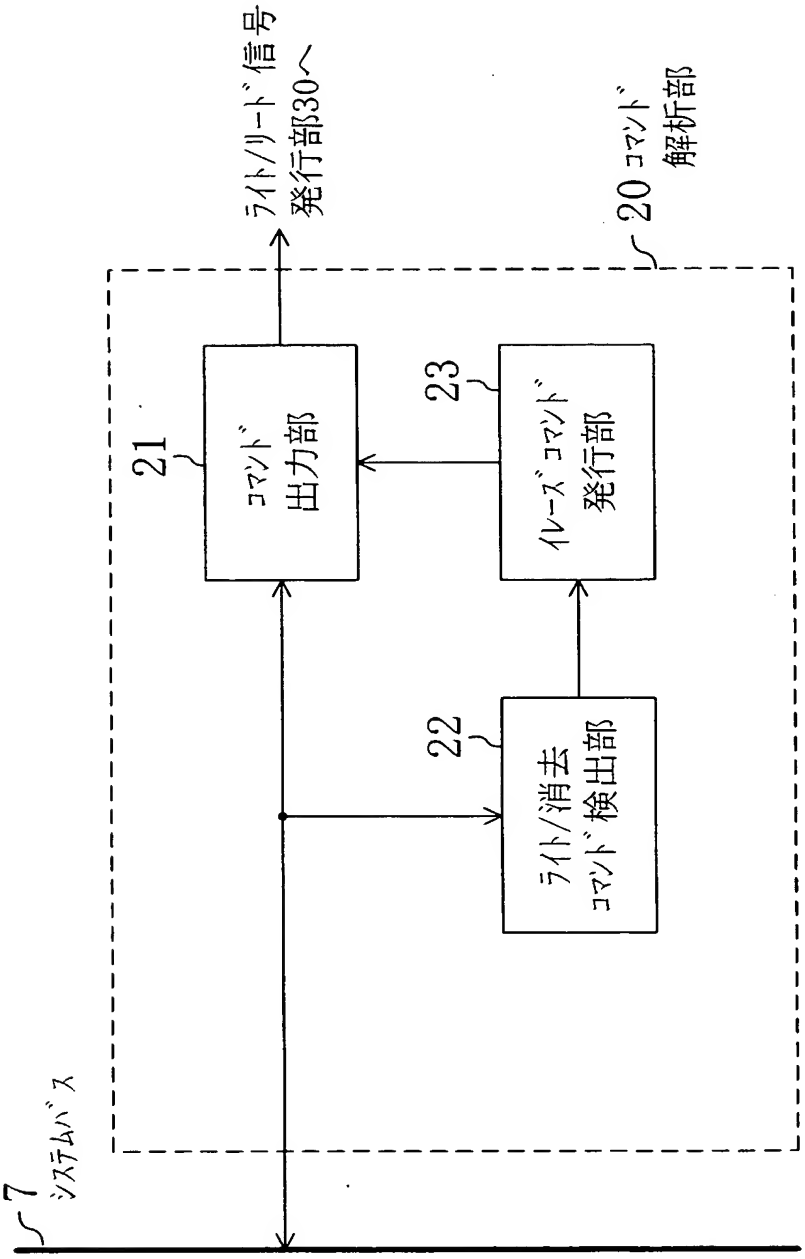
【図６】


20
状態1
状態2
状態3
状態4.1
状態4.2
状態5
状態6
全ての状態
ADRS=555h
DATA=AAh
ADRS=2AAh
DATA=55h
ADRS=555h
DATA=A0h
ADRS=555h
DATA=80h
ADRS=555h
DATA=AAh
ADRS=2AAh
DATA=55h
ADRS=各状態で示す以外
DATA=各状態で示す以外

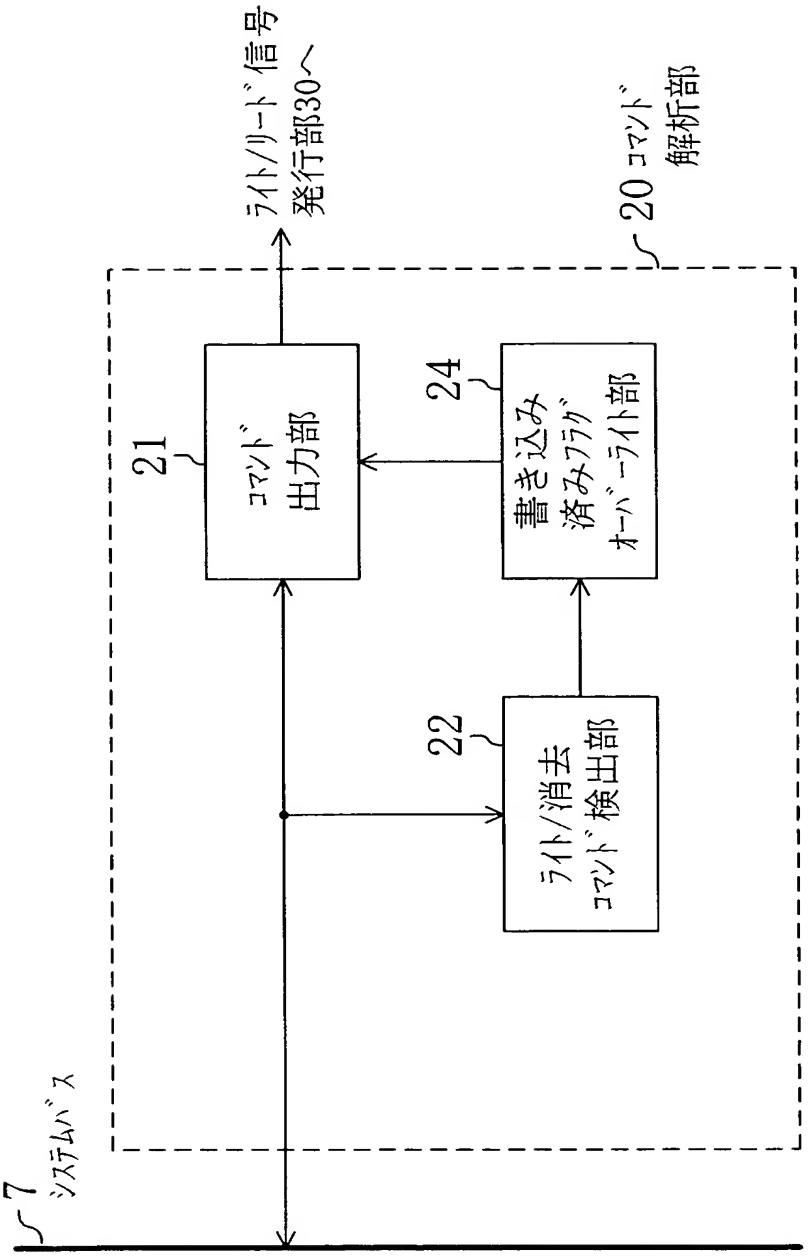
【図７】


6
0000h
0010h
ﾀﾞﾐｰﾊﾞｲﾄ
ﾀﾞﾐｰ
ｾｸﾀ
書き換え可能
領域
7FFFh
8000h
書き換え禁止
領域
7 6 5 4 3 2 1 0
FFF0h
F
FFFFh
8ﾋﾞｯﾄ

【図８】


ライト/リード信号
発行部30へ
20 ｺﾏﾝﾄﾞ
解析部
21
ｺﾏﾝﾄﾞ
出力部
23
ｲﾚｰｽﾞｺﾏﾝﾄﾞ
発行部
22
ライト/消去
ｺﾏﾝﾄﾞ検出部
7
ｼｽﾃﾑﾊﾞｽ

【図９】


ライト/リード信号
発行部30へ
20 コマンド
解析部
21
コマンド
出力部
24
書き込み
済みフラグ
オーバーライト部
22
ライト/消去
コマンド検出部
7
システムバス

【書類名】　要約書

【要約】

【課題】　システム作成者が改竄防止を必要とする情報の書き込みを自由にでき、かつ当該情報の改竄を確実に防止できる不揮発性メモリのアクセス制御システムを提供する。

【解決手段】　ブートＲＯＭに格納したシステム初期化のためのプログラムに従ってＣＰＵが不揮発性メモリ６上に書き換え禁止領域を設定し、かつ当該書き換え禁止領域上に設定した書き込み済みフラグＦに従ってアクセス制御回路が書き換え許可／禁止の制御を行う。

【選択図】　図２

特願２００３－０７５７１４

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社